Deutsche Bank

Non-Group Policy

South Africa Privacy Policy

Table of Contents

0. Key Data

Summary

This policy describes how DBSA"[1]"collects, uses, discloses and protects personal information.

Addressees

The policy is directed at all clients, third party service providers of DBSA and any other person whose personal information may be processed by the DBSA, such as prospective clients.

Implementation Date

3 July 2020 version 2 (revised September 2021)

[1] DBSA refers to Deutsche Bank AG, Johannesburg Branch, Deutsche Securities Pty Ltd and Deutsche Securities South Africa Pty Ltd.

1. Scope

DBSA cares about protecting the personal information entrusted to us. This policy describes how we collect, use, disclose and protect personal information. Personal information means information about a **living natural person and a juristic person** (each a "person") to which privacy and data protection legislation in South Africa applies and as may be more particularly defined or limited by such legislation.

2. Collection

We collect personal information directly from you, the corporate or institutional client, vendors and others and where lawful and reasonable, we may collect personal information about such persons from third parties and publicly available sources. We also collect personal information by CCTV cameras for security purposes, for any purpose relating to the prevention or curtailing of a disease or a pandemic and to comply with requests from legal and foreign regulators.

We use personal information to:

- Manage risk, detect and prevent fraud, to meet the requirements of anti-money laundering and terrorist financing laws and regulations and other legal, regulatory and industry self-regulatory requirements. These purposes may lead us to (among other measures):
  - establish and verify your and our clients' identity, confirming politically exposed person status and check it against money laundering, terrorist financing or similar watch lists established by regulatory agencies or similar bodies in South Africa and internationally; and
  - check and evaluate prospective clients' and business principals' past dealings or accounts with us or our international branches and affiliates, including, for example, information about on-boarding rejections, relationship terminations, suspicious financial activity reports and other information material to financial risk assessment and fraud prevention, generally using a person's personal information to protect DBSA and its employees from fraud and error.
- Comply with legal reporting requirements stipulated by legislation, in country and cross border;
- Customer profiling;
- Maintain business records for reasonable periods and to meet legal and regulatory record retention requirements;
- Meet our responsibilities to you and/or our clients;
- Follow your and/or our clients' instructions;
- Tell you and/or our clients by telephone and/or electronic communication about services and products available within the Group;
- Make sure our business suits client needs;
- Maintaining employee records as to Group requirements and for reporting purposed to the Department of Labour;
- Cross-check your qualifications and experiences with the requirements of job positions either currently vacant or becoming vacant in the future;
- Conducting background checks, including criminal records and ITC;
- Maintain a record of visitors to our premises for the means of corporate security as well as Occupational Health and Safety;
- Complete all requirements stipulated by Deutsche Bank Vendor Risk Management Policy; and
- Otherwise with a person's consent, or as permitted or required by law.

Without personal information, we may not be able to provide or continue to provide our clients with the products or services that they need.

DBSA is part of the Deutsche Bank Group and detail on the Group's data privacy rules can be found at the below external web address

https://www.db.com/company/en/data-protection.htm

3. Your/client consent

Consent to the collection, use and disclosure of personal information may be given in various ways.

Consent can be express (for example, orally, electronically or on a form signed describing the intended uses and disclosures of personal information) or implied (for example, when you and/or a client provides information necessary for a service requested). You may provide your consent in some circumstances where notice has been provided to you about our intentions with respect to your personal information and you have proceeded to obtain our products or services or have not withdrawn your consent for an identified purpose, such as by using an "opt out" option provided, if any. Consent may be given by your authorized representative (such as a legal guardian or a person having a power of attorney). **By providing us with your personal information, we will assume that you consent to our collection, use and disclosure of such information for the purposes identified or described in this Privacy Policy, or otherwise at the time of collection. Therefore, by providing personal information to DBSA, you consent to us processing your personal information as set out in this policy.**

If you provide us with personal information about another person, we will assume that you have the consent of that individual or entity to enable us to collect, use or disclose their personal information to us as described in this Privacy Policy.

You may withdraw your consent to our collection, use and disclosure of personal information, subject to contractual and legal restrictions and reasonable notice, and provided that any consent you have given for certain purposes (for instance, risk management, fraud prevention and similar legitimate purposes identified in this policy) will be valid for so long as necessary to fulfil those purposes. Note that if you withdraw your consent to certain uses of your personal information, we may no longer be able to provide certain of, or all of, our products or services. Consent cannot be withdrawn in relation to the provision of a credit facility after credit has been granted. Even if you withdraw your consent, DBSA will still process personal information if it is legally entitled to do so.

DBSA generally intends to collect, use and disclose your personal information with your consent, except as permitted or required by law. We may be required or permitted under statute or regulation to collect, use or disclose personal information without your consent, for example, to comply with a court order, to comply with local regulations or a legally permitted inquiry by a government agency, or to enforce our rights.

4. KYC Information

The following KYC information is gathered by the Client On-Boarding team and is mandatory in terms of the FIC Act 1 0f 2017.

Activity	What Data is being Received or Requested	Reason for the Data being Received/ Requested	Source of the Data

KYC Client Adoption; Maintenance and Closure	> Client (Juristic Persons) - Personal Information and/or Supporting Documents > Related Party (natural persons)- Personal Information and/or Supporting Documents for natural persons > Ownership Information (Juristic and natural Persons)- Personal Information and/or Supporting Documents > Client Business information such as location of operations; industry; location of clients > Sanctions list checks > PEP and Adverse Media Checks	> To meet internal policies and procedures for client adoption and continued business relationship periodically	> Client; > 3rd Party repositories; > Independent 3rd parties; > Global Sanction Lists; > Public Domain (regulator websites etc.)
Product Adoption	> Client Business information such as location of operations; industry; location of clients; reason for product and how does it meet its own business imperatives > Agent (Juristic Person) - Personal Information and/or Supporting Documents as well as Investment Management Agreement and/or Mandate to document agency agreement	> To meet internal policies and procedures for client adoption and continued business relationship periodically	> Client; > 3rd Party repositories; > Independent 3rd parties; > Global Sanction Lists
Regulatory Queries received internally	> Client Existence > Client data/ documents > Client PEP data	> To meet bank regulatory responsibilities	> Internal KYC repository

Regulatory Audit	> Client (Juristic Persons) - Personal Information and/or Supporting Documents > Related Party (natural persons)- Personal Information and/or Supporting Documents for natural persons > Ownership Information (Juristic and natural Persons)- Personal Information and/or Supporting Documents > Client Business information such as location of operations; industry; location of clients > Sanctions list checks > PEP and Adverse Media Checks	> To meet bank regulatory responsibilities	> Internal KYC repository

5. Third parties/Service Providers

Personal information may be transferred to, or collected by, affiliates/associates, third party agents or service providers we engage to provide services on our behalf, including administrative, billing, compliance, reporting, information technology or other processing or custodial services. Some of these entities may be located outside of South Africa, including, without limitation, in the United States, the United Kingdom, Singapore, India and Germany. These countries may not have data-protection laws similar to those in South Africa.

We take reasonable measures to ensure that any personal information that may be collected, used, disclosed or otherwise processed by these service providers, agents and/or our affiliates/associates on our behalf is protected and not used or disclosed for purposes other than as directed by DBSA, subject to legal requirements in foreign jurisdictions applicable to those organizations, for example lawful requirements to disclose personal information to government authorities in those countries.

If you wish to access written information about our policies and practices with respect to service providers outside South Africa, please consult this Privacy Policy. If you have any questions about the collection, use, disclosure or storage of personal information by a service provider outside South Africa on behalf of DBSA, please contact our Information Officer- Johan Gibhard
johan.gibhard@db.com Tel: 27 (0)117757456

6. Recording of Telephone Calls

We may monitor and/or record telephone conversations with our representatives for our mutual protection, to ensure that client instructions are carried out, to document DBSA's compliance with legal requirements and to ensure that service levels are maintained. We may also use voice-recognition to enhance the customer experience, detect fraud or for other purposes relating to our business.

7. Surveillance Cameras and Recording

We may monitor movement in and around our premises by closed-circuit television for our mutual security and protection, including to safeguard our domiciliary right and to collect evidence in cases of robbery and fraud. We may also use face recognition techniques to identify perpetrators of wrongful or criminal acts.

8. Storing personal information/Security

We protect personal information using physical, electronic or procedural security measures appropriate to the sensitivity of the information in our custody or control, which may include safeguards to protect against loss or theft, as well as against unauthorized access, disclosure, copying, use or modification. Authorized employees, agents and third-party service providers of DBSA who require access to your personal information in order to fulfil their job requirements may have access to your personal information.

Our security systems are designed to prevent loss, unauthorized destruction, damage and/or access to your personal information from unauthorized third parties.

How long will your data be stored for?
We may store personal information unless you object, but we usually store it for as long as we are legally obliged to do so. If you object, we will only store it if we are legally permitted or obliged to do so.

9. Marketing by electronic or telephonic means

We may use personal information to inform you of our products, market trends, economic outlooks etc. If you later decide that you do not want us to do this, please inform us accordingly by contacting our Information Officer.

10. Monitoring of electronic communications

We communicate with you through different methods and channels. Where permitted by law, we may record and monitor electronic communications to make sure that they comply with our legal and regulatory responsibilities and internal policies.

11. Your rights

We will take note of your rights under applicable privacy and data protection laws, especially your right to object, on reasonable grounds, to certain types of processing.

You have the right to query a decision that we make about a product or service that you have applied for and that was made solely by automated means by contacting the Information Officer or appeal to the Regulator.

Please note that even if you object to certain processing of Personal Information, we may still continue this processing if permitted or required to do so by law, for example to enable us to fulfil legal requirements, administer the employment or fulfil obligations under a contract with you.

You also have the right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator can be found below.

Website: https://www.justice.gov.za/inforeg/

Address:

33 Hoofd Street

Forum III, 3rd Floor Braampark

P.O Box 31533

Braamfontein, Johannesburg, 2017

Mr Marks Thibela

Chief Executive Officer

Tel No. +27 (0) 10 023 5207, Cell No. +27 (0) 82 746 4173

inforeg@justice.gov.za

12. Right to change this Privacy Policy

This Privacy Policy may be revised from time to time. If we intend to use or disclose personal information for purposes materially different than those described in this policy, we will make reasonable efforts to notify affected persons, if necessary, including by revising this Privacy Policy. The policy will be published on our website at https://country.db.com/south-africa/documents/Privacy_Policy_South_Africa.pdf?language_id=1

If you are concerned about how your personal information is used, you should contact us as described above to obtain a current copy of this policy. We urge you to request and review this Privacy Policy frequently to obtain the current version. The publication on our website and/or your continued use of our products and/or services and/or continued provision of personal information would constitute your acceptance of changes to the policy.

13. Data minimisation

We will use Personal Information only when it is necessary for and relevant to fulfil a particular internal process, task or project. If we cannot avoid using Personal Information, we will only use the particular information necessary for the intended, legitimate purpose. In particular:

- We will limit the Personal Information we share with others, both internally (including with other DB entities) and externally, to that which is expressly authorized to be shared; and
- We will not record information about people in emails, instant messages, or free text fields in databases, which is not required for business purposes.

14. Data accuracy

Personal Information will be kept accurate, complete and up to date. You undertake to only provide accurate and up to date Personal Information to DBSA and to inform us without delays of any changes. You as a data subject provider would be liable for any loss incurred or damage suffered by DBSA for relying on inacurate information.

If we notice any inaccuracies in the Personal Information that we handle, or if an individual or entity notifies us of an inaccuracy or change in their Personal Information, we will correct these immediately or escalate to the relevant person/team to be rectified.

Each internal business division and infrastructure function will ensure that it has adequate procedures in place to amend incorrect information and document that correction has been completed.

15. Data sharing

Personal Information will only be shared on a 'need to know' basis. This means that information about individuals and entities will not be disclosed to anyone who does not have a legitimate need to receive or access it. This applies when dealing with colleagues internally and with external contacts. This includes sending information to regulators on request which might inadvertently contain information on 3rd parties, i.e., information on individuals and entities gathered for legitimate purposes.

The above clause is qualified to confirm that we will use reasonable endeavours to only share Personal Information on a need to know basis or if we are lawfully permitted to share the data.

Each internal business division and infrastructure function will have appropriate processes in place to validate access permissions or participate in central recertification processes.

Where Personal Information is disclosed to a vendor (e.g., a service provider to DB), only Personal Information necessary will be disclosed. In addition, the agreement with the vendor will contain appropriate data protection provisions to ensure that the vendor complies with our requirements for Processing Personal Information.

16. Rights of individuals and juristic persons

Individuals and entities are granted the below rights in terms of POPIA and we will adhere to these rights:

- the right to be informed about how and why their Personal Information is used;
- the right to ask for copies of the Personal Information held (including information contained in emails, instant messages, notes etc.);
- the right to ask for any inaccuracies in their Personal Information to be corrected;
- the right to have their Personal Information erased (where no obligations to keep the data exist beyond the retention period). You may also request that your Personal Information be erased if e.g. the Personal Information is no longer necessary for the purposes for which it was collected, if the processing is based on your consent and you withdraw your consent for a specific process and there is no other legal ground for processing your Personal Information, if you object to the processing of Personal Information where we do not have an overriding legitimate interest, the processing is unlawful, or the Personal Information has to be erased to enable us to comply;
- the right to ask to stop Processing their Personal Information;
- the right to object to their Personal Information being used for direct marketing purposes;
- the right to have any Personal Information that they have provided to be transferred to another party ; and
- the right not to be subjected to a fully automated decision-making process (i.e., a system generated decision without any human input), where the outcome has a legal, or similarly significant effect on the individual concerned.

When an individual or entity exercises any of the above rights, we will respond to the request in a strict time frame (in many cases one month, meaning one month to carry out the requested action).

Each business division and infrastructure function will maintain procedures to facilitate such requests from individuals and to ensure they are dealt with promptly (or rejected after review).

17. Compliance

All internal Business and Infrastructure heads are personally responsible for implementing and maintaining respective control standards and governance procedures to ensure compliance with this policy.

18. Glossary

Term	Definition
consent	means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
direct marketing	means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: (a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or (b) requesting the data subject to make a donation of any kind for any reason.
electronic communication	means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.
filing system	means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.
information officer	of, or in relation to, a: (a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17 of the Promotion of Access to Information Act; or (b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act. Johan Gibhard- johan.gibhard@db.com Tel: 27 (0)117757456
person	means a natural person or a juristic person
personal information	means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a privat or confidential nature or further correspondence that would reveal the contents

Term	Definition
	of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
POPIA	means Act No. 4 of 2013: Protection of Personal Information Act, 2013
processing	means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including— (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of Information.
public record	means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.
record	means any recorded information: (a) regardless of form or medium, including any of the following: (i) Writing on any material; (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; (iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; (iv) book, map, plan, graph or drawing; v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; (b) in the possession or under the control of a responsible party; (c) whether or not it was created by a responsible party; and (d) regardless of when it came into existence.
Regulator	means the Information Regulator established in terms of section 39 of POPIA;